This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A2

(11) International Publication Number: **WO 99/49379**

(43) International Publication Date: 30 September 1999 (30.09.99)

(21) International Application Number: PCT/US99/04937

(22) International Filing Date: 5 March 1999 (05.03.99)

(30) Priority Data:

60/077,136	6 March 1998 (06.03.98)	US
60/082,772	23 April 1998 (23.04.98)	US

(81) Designated States: CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

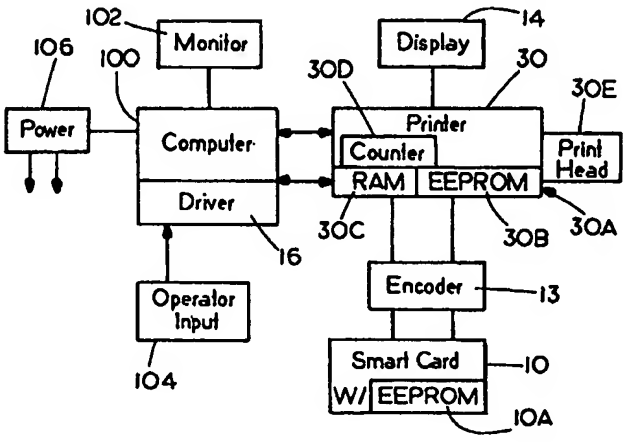
Published
Without international search report and to be republished upon receipt of that report.

(71) Applicant: FARGO ELECTRONICS, INC. [US/US]; 6533 Flying Cloud Drive, Eden Prairie, MN 55344 (US).

(72) Inventors: FRANCIS, Robert, E.; 6828 Morgan Avenue South, Richfield, MN 55423 (US). DUNHAM, Matthew, K.; 3877 Kennet Circle, Eagan, MN 55123 (US). KLINEFELTER, Gary, M.; 18763 Erin Bay, Eden Prairie, MN 55347 (US). IBS, Jon, J.; 4827 Chicago Avenue South, Minneapolis, MN 55401 (US).

(74) Agents: WESTMAN, Nickolas, E. et al.; Westman, Champlin & Kelly, P.A., International Centre, Suite 1600, 900 Second Avenue South, Minneapolis, MN 55402–3319 (US).

(54) Title: SECURITY PRINTING AND UNLOCKING MECHANISM FOR HIGH SECURITY PRINTERS



(57) Abstract

A printer (30) is provided with a smart card (10) encoding device (13) that is externally accessible. The smart card (10) is a key with an integrated circuit (50) including a memory (10A) that will retain a discrete password and other digital information. The password on the smart card key (10) must be compared to a password stored in the printer memory (30A, 30B) before printing operations will be permitted. The digital information in the smart card key memory (10A) can include marks (122) or graphics that would indicate that the cards being printed (120) by the printer (30) are secured cards and authorized cards. The information will be printed from the smart card key memory (10A) only when the passwords match so that the discrete information on the smart card key (10) can be used for driving the printer (30) for printing this information. The printer (30) is made into a high security printer by permitting overriding of the password only upon the generating of identical numbers from separated algorithms, one in the printer memory (30A) and one at a secure location. An algorithm input is a dynamically changing parameter of the printer (30), such as the number of print head (30E) passes, or the number of cards (120) printed so the algorithmically generated numbers are unique.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SECURITY PRINTING AND UNLOCKING MECHANISM FOR HIGH SECURITY PRINTERS

BACKGROUND OF THE INVENTION

The present invention relates to using a smart card key for high security printers and insuring access only when a unique password is provided as well as printing markings from information stored in the smart card key memory.

Smart cards, which are identification cards made from the traditional poly vinyl chloride/polyester cards having an integrated circuit embedded in the card, allowing for information to be stored in the card itself, are widely used. Typically the integrated circuit consists of either a memory or a microprocessor with memory. In order for a smart card to be encoded in the printer, the printer must have a smart card encoder.

One of the problems inherent in identification card printers is that anyone with access to the files or even to a inexpensive commercial drafting software program can recreate the identification card and print forgeries. This problem is particularly acute in locations where the printer, software, files, and other computer hardware are set up in a single area.

SUMMARY OF THE INVENTION

The present invention relates to maintaining security of a printer and its user by having a secure smart card key. The printer is, as shown, an identification card printer and has an externally accessible smart card encoder that can be used for initializing a smart card that forms a key. A further use of the externally accessible smart card encoder is to read the smart card and allow or prevent access. It is also possible to encode smart cards inside the

printer, if so desired, by placing a second encoding device in the internal printing path of the printer.

Because a smart card can have a large amount of memory storage, both a digital image (such as a security mark for cards to be printed) and passwords can be stored in the smart card memory. The printers also can have large capacity Electrically Erasable Programmable Read Only Memory (EEPROM), as well as read only memory (ROM).

The first password usage of the smart card key is to enable printing by a selected identification card printer. The second password usage is to enable printing a specialized print panel for a security mark using a stored digital image in the smart card key memory. The ability to enable password protected printing only is provided initially in a computer program for the printer drive computer which converts computer images into digital data for printing cards. The computer program or software includes user interface items for setting passwords, duplicating smart cards, and loading images onto smart card memory. In addition, the selected password would also be stored in the associated identification card printer memory.

A match between the password in printer memory and the password in the smart card key memory is required to enable printing as the basic security feature. Thus, the smart card would act as the only key to allow the printer to print. The ability to store a digital representation of a security mark to be printed onto an identification card being printed by the card printer controlled by the smart card key prevents unauthorized use of the security mark, since

accessibility to the mark is limited to the holder of the smart card key with the correct password.

Another aspect of the invention is an algorithmic unlocking mechanism available to users of the smart card key having a high security password feature, in case they ever lost the encoded smart card key or forgot the password. High security as used herein means that the password cannot be easily changed or bypassed. Printers are now equipped with a counter mechanism to count the number of passes that the printhead has made during the operation of the printer, or provide other changing counts. This number can be accessed and displayed on the display of the printer or the number can be printed on an I.D. card in the printer. The counter is a conventional system used in a wide variety of devices. In addition, other changing parameters in a printer can be used for a count, for example, a count of the number of cards printed in the printer can be recorded and used for this invention.

After a selected procedure by the owner of the printer, which verifies ownership of the high security printer, an algorithm is applied to the number generated by the counting mechanism. The algorithm is selected to produce an unlocking number unique to each number of the printer head pass count, a range of printer head pass counts or number of cards printed, as recorded by the counter in that printer. This can be done automatically by the printer if a smart card key used does not have an acceptable password. The count is based on a dynamic parameter unique to that particular printer. A duplicate algorithm to the one in printer memory is kept at a secure location, for example at the premises of the

printer manufacturer. The printer manufacturer, after verifying the identity of the owner through a personal identification number, will use the algorithm to generate a one time usable unlocking number.

The owner is then issued this one time usable unlocking number generated from the algorithm at the secure location, which is entered through the host computer in place of the password from the smart card key. The printer will apply or compare the unlocking number generated in printer memory with the number generated from the secure location. If the algorithmically generated number entered by the user matches the algorithmic unlocking number generated in the printer, then the printer will accept and perform the current command given to the printer, such as a command to create a new smart card key or to disable the security feature entirely, or to change the password.

Although the printer memory stores the algorithmic unlocking code, the stored code cannot be used to unlock the printer without the separate algorithmic application, using the same algorithm, but kept at site unrelated to the user, thus protecting the security of the printer. The security value is that the pass count number (or other unique number) from the counter mechanism of the printer is one that the user has no control over, is constantly changing, and cannot be manipulated.

Once the printer has continued to print and the number of printhead passes counted and stored in printer memory has changed, the previously generated unlocking number will no longer match the number produced by the algorithm in the EEPROM of the printer

after the change and therefore, the old number will not allow the printer to function.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic block diagram representation of a high security printer having a smart card key input as attached to a host computer;

Figure 2 is a perspective part schematic view of a typical printer having an encoding device on the exterior of and used with the present invention;

Figure 3 is a sectional view illustrating schematically a removable memory card key, as shown a smart card, in the encoding device;

Figure 4 is a plan view of the smart card key showing an integrated circuit exposed on one side thereof;

Figure 5 is a plan view of a typical identification card printed from a printer using the high security arrangement of the present invention;

Figure 6 is an overall flow diagram of operations carried out to accomplish the purposes of the present invention;

Figure 7 is a flow diagram for enabling printing of a security mark on an identification card based on a digital image stored in the smart card key; and

Figure 8 is a flow diagram of an off-site verification procedure for the high security printer of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Smart card encoding is well known in the identification card printer industry. Identification card printers such as the FARGO Cheetah II printer sold by Fargo Electronics of Eden Prairie, Minnesota have the capability of encoding smart cards. However,

the Cheetah II printer encodes smart cards internally rather than having the encoder externally accessible. As shown herein the smart card is removable and is thus usable as a key for operating a device that is controlled to perform some operation, such as a printer.

In Figure 1, the general layout of usable, typical components is shown. A computer 100 is connected to a controllable device having a memory, as shown a printer 30, and is used for the initial and subsequent programming. A monitor 102 can be used for the display menus from a software program for encoding a removable memory device key, as shown a smart card key 10, through the input slot on the printer for an encoder 13 as will be explained. Operator inputs from a keyboard 104 are used for selecting the functions, and a power supply 106 is used for powering both the computer 100 and the printer 30. The software for the control of the security features of the present invention is installed in the computer in a normal manner, including a CD to provide the necessary programming for enabling smart card key 10 and providing a selected password that is entered in the smart card key memory 10A. As will be shown, the smart card key is slid into a slot 12 (Figure 2) in printer 30 and the smart card key 10 contains an embedded integrated circuit 50 (Figure 4) chip that has integrated circuit contacts accessible from the exterior. The contacts will complete circuits from the printer or computer to the memory on the chip.

The removable memory device, as shown a smart card with external contacts 10, can be a contactless smart card, a radio frequency (RF) identification card, a PCMCIA card, or a compact

"flash module" (used currently in digital photography) or any other type of removable memory device. Thus, the encoding device does not need contacts if a contactless removable memory device key is used. This description will show a contact arrangement with for the smart card key.

The computer 100 will be used to select a particular printer 30 that is being used, and in which the card key 10 is inserted. The initializing menu from the program will have prompts that will include a prompt for entering a password selected by the user, and for example up to an eight character password using any standard alphanumeric keyboard characters is entered. Once the password is entered, it can be confirmed by typing it again into a "confirm" password box presented by the menu.

If the smart card key 10 is being used with multiple printers, it can be encoded appropriately with just the password for identification, but if the smart card key 10 is used with only one printer, it will receive and retain in memory the printer serial number, along with the encoded password to a specific smart card key, making all other access cards or key cards created in other printers invalid. If more than one printer is utilized, then each printer can be enabled with the same password.

Once the password has been entered into the computer 100, it will be passed through the printer memory indicated at 30A, from driver software 16 to the card 10, and imprinted in an electrically erasable programmable read only memory (EEPROM) 10A of the chip 50 on the smart card key 10.

Once the smart card key has been programmed with a password, it can only be changed under certain

selected circumstances or conditions, and these are controlled as desired from the computer 100, but require information separate from the computer to be operated. Generally it will be necessary to have the card 10 in the printer 30 and then connected to the computer 100 for changing the password and only when the correct password match between the card memory 10A and printer memory, unless the unlocking algorithmic procedure to be described is followed.

Additionally, if desired, the card printer 30 can be used to print a security image or mark onto cards that are being printed using a special ribbon layer. The printing of the security mark is controlled from a digital image program that is entered in the EEPROM 10A of the smart card key 10. This digital image can be entered from the software program of computer 100 for inputting information into the EEPROM 10A, and the image, such as that shown at 122 in Figure 5 on an identification card 120 printed on printer 30, can only be viewed when the card is tilted slightly for reflecting light. These security mark images can be made to glow when viewed under an ultraviolet light. The image 122 can be put any place on a card that is to be printed as desired. The storing of the security mark or image in the smart card key memory only insures that such image or mark will only be printed when the correct smart card key is used, since the printer 30 will not operate until the password on that key 10 matches the printer password.

The digital input to print such an image, and other security features are in the EEPROM 10A on the card only. After entry of the information, the

inputted digital file for the image is deleted automatically or manually.

The printer driver software 16 can be imbedded in a microprocessor in the printer if desired, and the use of the card 10 for enabling a printer 30 can be done with the printer 30 standing alone, and powered. The printer 30 will normally be used with the computer 100, but the printer includes memory of its own (both ROM and EEPROM). Once the password is entered into the printer memory, the printer memory will perform the needed functions.

Upon receiving a "print" command, the printer memory determines whether or not the security feature has been enabled on the controlled device, as shown the printer 30. If the security feature has been enabled, then the removable memory device card, as shown smart card key 10, must be present in slot 12, and if so, then the memory in the printer will interrogate the card 10 to determine the password in memory on the card and compare it with the password that is in the printer memory. Only if the password matches, will the printer operation be undertaken. Figure 3 depicts a smart card 10 that is provided with an integrated circuit chip 50 having a password in memory.

A smart card key 10 is placed into slot 12 in printer 30. The encoder 13 used to initialize and read the smart card key 10 is thus externally accessible as shown in Figure 2. The control panel 11 of the printer 30 has an LCD display 14 and command buttons 15. The smart card key memory chip 50 can be read through external or export contacts 52. The contacts 52 are engaged by spring loaded contacts 13A in the encoder slot. The coupling to the smart card

key memory 10A is made as the card is "clicked" into place. Insertion of the smart card key 10 with the integrated circuit facing the correct way through the slot 12 allows contacts to complete circuits to the memory on chip 50, which is encoded electronically.

The contacts 52 are used for initially placing information into the integrated circuit memory of chip 50 as well as reading stored information. The commands are generated in the computer 100 or printer 30 in a normal manner, and for printing can be processed through the printer memory.

Commands are presented in a flow chart in Figure 6. Each particular printer, in order to interface with any software program run on a computer must have a printer driver 16 to provide the link up to the computer. The driver 16 forming part of computer 100 provides the operator with a menu of choices, as shown, disable password 17, enable password 18, change password 19, duplicate password 20, and set up security shield 21. The operator will choose which menu option is utilized to download corresponding information to the smart card key 10 in a conventional routine.

In order to initially provide a smart card key memory with a digital image of a security mark, such as a logo stored digitally in the memory of the smart card, the operator must choose the "set up security shield " menu step 21. The driver program 16 in the computer controlling the printer then requests position information at step 26 and gives the operator options for positioning the shield or mark at step 27. The positioning is information about the location of the security mark on the identification card 120 in Figure 5 that is printed in the printer 30.

Figure 5 shows a printed Identification Card 120 with a digital image or security mark 122 that can be printed in various locations on the identification card. These locations can be varied by changing the location in software located in the computer 100 attached to the printer 30. The number of digital images can also be varied by changing the number of digital images created in software located in the computer attached to the printer.

From a graphics software application in computer 100, where the digital image of a mark has been constructed, the operator selects the "select security shield " step 37 from the printer setup in the graphic application and then chooses print step 38 from the graphics application. The print command step 38 will start the process to transmit both the digital image and the location information to the smart card key 10 memory, rather than commanding the printer to print, when the security shield mode at step 37 has been selected.

Next, the image seal is processed into the appropriate format at step 28, and then transmit the digital image and settings at step 29 to the printer 30. The printer 30 then transmits the image and settings at step 31 to the smart card key integrated circuit memory 10A via the smart card key encoder 13.

It would be possible for a skilled practitioner to create a separate program specifically written to enable the transfer of the digital image data and location data within the teachings of the present invention.

To enable (create) a password or to make changes in the password, other menu options are used at the computer 100, as provided by software in the

computer. The password information is to be stored in the memory on the same smart card key 10 as that used for storing the digital image to be printed by printer 30 as just described. In order to place a password onto the smart card, key 10, the "enable password" menu option 18 must be chosen. The computer driver program then prompts the operator to enter the selected password at step 22 and confirm the password at step 23 as was previously mentioned.

The operator then has the option to make the smart card specific to a single printer by choosing the "yes" option of the printer specific card prompt at step 39. The printer 30 has an Electrical Erasable Programmable Read Only Memory (EEPROM) that contains a serial number for that printer that can also be encoded into the smart card key memory through encoder 13. Once encoded to the key memory, the printer serial number would be compared in the same manner as the passwords, which would prevent the printer 30 from printing unless both the password and the serial number matched. The password from the smart card key 10 is then transmitted as a send command 32 to the printer 30 where the printer memory decodes the message at step 33, verifies the password, step 34, and executes the command message at step 35 if the printer is enabled by the correct password.

To change the password, the operator must insert the smart card key 10 into the encoder 13, then select the "change password" menu option 19 from the software in the computer 100. The current password must be entered as shown by step 36. The operator is prompted to enter the new password as at step 24 and confirm the new password as at step 25. The new password is then transmitted as a send command at step

32 to the printer 30 where the printer decodes the message at step 33, verifies the password, step 34, and executes the command message step 35.

To duplicate the password as shown at menu option 20, the operator must insert the originally encoded smart card key 10 into the encoder 13, then select the "duplicate password" menu option 20. The current password must be entered at step 22A to verify that operation is authorized and the change can be made. The password is then transmitted as a send command at step 32 to the printer 30 where the printer memory decodes the message at step 33, and verifies the password at step 34. Then the printer driver prompts the operator to remove the original smart card key 10 and place a new smart card key 10 into the encoder 13. The printer 30 then executes the command message at step 35. The changes can be made only if the original password on the smart card key 10 has been entered.

To disable the password, the operator must insert the smart card key 10 into the encoder 13, then select the "disable password" menu option 17 at the computer 100. The current password must be entered at step 22B and the password to be disabled is then transmitted as a send command 32 to the printer 30 where the printer decodes the message at step 33, verifies the password at step 34, and executes the command message at step 35.

It would be clear to a skilled practitioner in the art that these commands could be structured in a variety of permutations. Any of those known permutations may be used as long as security is maintained.

Once the smart card key 10 has been encoded, the password encoded on the smart card key 10 can be stored in the printer EEPROM 30B. The EEPROM 30B on the printer 30 also contains the unique serial number for that printer. When an operator has encoded the smart card key 10 and wants to print, the operator reinserts the smart card key 10 into the encoder 13. The printer 30 then copies the information contained in the integrated circuit memory of the Smart Card to the printer's Random Accessible Memory (RAM) 30A. The printer RAM 30A then compares the password and, if the option of making the smart card key 10 specific to one printer has been chosen, the RAM compares the serial number on smart card key 10 to the password and serial number retained in the printer EEPROM 30B. If the passwords in both memory locations (card and printer) match, then the printer 30 will enable the print commands to proceed. The printer will continue to allow the print commands until the smart card key 10 is removed from encoder 13. Once the smart card key 10 is removed from the encoder 13, the same process has to be repeated for the printer 30 to start printing again.

When an operator has encoded the smart card key 10 with a digital image such as a logo and wants to print identification cards that contain the logo such as that shown at 120 in Figure 5, the operator must reinsert the smart card key 10 into the encoder 13. The printer 30 then copies the information contained in the integrated circuit memory on the smart card key 10 to the printer's Random Accessible Memory (RAM) 30C. The printer memory then compares the passwords and, if included, the serial number from card key 10 to the passwords and serial number

retained in the printer EEPROM. If correct, the printer stores the digital image and the location information transmitted from the smart card key 10 in the RAM memory. The printer is programmed to check to see if the ribbon with the specialized security mark panel is loaded into the printer 30, and if the correct ribbon is loaded, and if the passwords in both memory locations match, the printer will commence the print cycle. The printer will continue to allow the print commands until the smart card key 10 is removed from encoder 13. Once the smart card key 10 is removed from the encoder, the same process would need be repeated for the printer 30 to start printing again.

A practitioner skilled in the art would be able to discern that saving the password in the computer or not saving the password at all and requiring the operator to enter the password each time that the operator used the printer 30 could accomplish the same increase in security of the printer 30 within the scope of the present invention.

A counting device or counter 30D (Figure 1) is added to either a circuit board in the printer or to the print head mechanism itself for counting the number of passes of the print head 30E during printing or counting the number of cards. An electronic counting device or counter in printer memory would be the preferred embodiment but other counting devices such as a mechanical counting device could be used for recording a changing event as printing progresses.

In every instance where the printer is given a command, the process shown in Figure 7 occurs. The command step 40 is given to the printer 30. The printer 30 memory determines if the printer is

security enabled at step 41. If the answer is no at step 42, (no security check is needed) the printer 30 proceeds with the command as at 43. If the answer is yes at step 44, then the printer 30 determines if the smart card key 10 is inserted into the slot 12 of the encoder 13 and if the correct password is encoded onto the smart card key at step 45. If the answer is yes at 46, the printer memory then determines if the user password is needed at step 47 and matches the password in the printer EEPROM 30B. If the password is not needed as at step 48, the printer proceeds with the command given, step 49. If the password is needed and matches, then the printer proceeds with the command at step 51.

If the printer memory determines that the smart card key 10 is not inserted into the slot 12 or if the incorrect password is encoded onto the smart card key memory, at 45, or if the user password is needed as at step 47 and the password on key 10 does not match the password in the printer EEPROM, then the printer 30 automatically runs an internal check of the print head pass count at step 54 using the counter. The printer algorithmically processes the print head pass count at step 45 using an algorithm stored in printer memory to get a unique internal unlocking code number. The printer memory then compares the internal unlocking code number to the user entered password on the key 10 at step 56.

This separate code number can also be derived from a duplicate algorithm kept apart from the printer, which also uses count of the events counted by the printer. If there is a match at step 57 between the internal unlocking code number and the user entered password (or unlocking number), then the

printer will proceed with the command at step 58. If there is not a match at step 59 between the printer internal unlocking code number and the user entered password, then the printer will abort the command at step 60 and remain locked.

In the event that a user loses the encoded smart card key or misplaces their password, the unlocking process in Figure 10 is followed. As part of the present invention, users encoding the smart card key or enabling the password protection features of the printer contact an off-site verification location and can send a Personal Identification Number (PIN). PIN numbers are commonly used in such applications as ATM machines and for credit cards. PIN applications are well known in the art. Once a PIN number has been established, the user would have to verify the PIN number at step 61 or give some unrefutable evidence that the user is entitled to use that printer before any assistance in unlocking the printer would be given. When the user identification process is completed, the user is given a command from the off-site location that allows the print head pass count (or other count) to be displayed on a display 14 or printed on an identification card in the printer, at step 62. The print head pass count is then displayed at step 63 either on the LCD display 14 or on the identification card. The user relays the count selected to the off-site location at step 64. The off-site location is anticipated to be the headquarters of the printer manufacturer. The print head pass count is then put through the same algorithm as at step 55 which is contained in the printer. The resulting unlocking number at step 56 is then given back to the printer operator 65. The printer operator

then enters the unlocking number in place of the user password which starts the internal printer process as described above.

In summary, for unlocking a printer in case of a lost card, the memory in the printer contains an algorithm, which is a number generating algorithm that will provide a discrete output number based upon an input number the value of which outside the control the operator of the printer, such as a count of the number of print passes or cards printed, which count can be done with an internal counter in the printer. These numbers can be shown on a display on the printer, upon a command from the operator (which command also may be known only to the manufacturer) and using the algorithm and the variable number, the printer can generate a dynamically changing security number or password.

If the password on the smart card key does not match the password in printer memory, the memory in the printer can provide the algorithmically generated password automatically to see if it matches an override password. The override can be inputted from the computer 100, if desired, and if the algorithmically generated number in the printer is matched, then the printer can be operated, and can be used without a password or a new smart card key can be encoded with a new password that is generated.

The algorithm used is discrete for each particular count, and this permits a party that has lost a smart card key or password to call to the manufacturer, (or other off-site locations) who has the algorithm in memory identified by the printer serial number, and upon identification of the user, the user can provide the count that is used as an

algorithm input, and the off-site manufacturer then can run the algorithm with that discrete count inputted and provide a number that can be used as a separate auxiliary security unlock. This number can be put into a smart card key that would be provided to the user, or can be generated in the computer 100 for comparison with the algorithmically generated number from the printer memory using the same algorithm as that used by the manufacturer. A match then also will disable the security system for operation and for encoding and accepting a new password on a new removable memory device or smart card key.

The algorithm can be a normal number generating algorithm based upon an input number that varies or changes as the printer is used.

The removable memory device or card can be provided with a password in memory so it is a key to permit operation of a printer or another controllable device that performs operations. The removable memory device or card is a key to operating the controllable device and permits operation only when the card is associated with the externally accessible encoder and a password match is made.

Although the present invention has been described with reference to preferred embodiments, workers skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method of providing a security key for a controllable device having internal memory comprising providing an externally accessible encoder on the controllable device coupled to the controllable device memory, providing a removable memory device having a programmable memory, programming a password into the memory of the controllable device and from the encoder into the memory of the removable memory device, and removing the removable memory device from the encoder for use as a key for the controllable device.

2. The method of claim 1 including programming the memory of the removable memory device with control functions for operations of the controllable device in addition to the password.

3. The method of claim 1, wherein said removable memory device comprises a smart card key used in connection with an encoder of a printer for unlocking the printer to permit operation.

4. A process of controlling printing of a digital image to be printed onto a substrate in a printer comprising creating the digital image on a drive computer for the printer, transmitting the digital image to an encoding device coupled to the printer, encoding the digital image onto a removable memory carrying device having an integrated circuit memory for receiving and holding the digital image.

5. The process of claim 4 further comprising providing the removable memory device to a printer input and reading the digital image from the removable

memory device into a printer memory as a print command.

6. The process of claim 4 further including providing a password in a memory of the printer coupled to the encoding device, which matches a password on the removable memory device, and permitting the digital image to be printed only when the password in the memory of the printer matches the password on the removable memory device.

7. The process of claim 4 further comprising deleting the digital image from the drive computer to create a unique digital image encoded onto the removable memory device.

8. The process of claim 5 including providing a password in a memory in the printer coupled to the encoding device, which matches a password on the removable memory device for enabling the printer and matching with the password in the memory of the printer and the password on the removable memory device prior to enabling the printer.

9. The process of claim 7 including providing a serial number in the memory of the printer, and encoding the serial number into the removable memory device, for comparison and matching serial numbers before enabling the printer.

10. The process of claim 4 including encoding an algorithm into the memory of the printer, using the algorithm for generating a number as a function of an input of a discrete number, the number generated by

the algorithm providing a secondary password for comparison with inputs to the printer memory.

11. The process of claim 10 and providing the same algorithm as in the printer memory at an off-site location, counting a discrete dynamically changing parameter in the printer as printing operations proceed, using the counter output for an input to the algorithm in the printer memory and in the same algorithm off-site to provide matching numbers based upon dynamically changing conditions of the printer.

12. The process of claim 4 including memory in the printer to identify presence of a removable memory device in the encoding device.

13. A process for unlocking a password protected secure printer comprising providing a printer that contains memory for comparing an internal password with an externally inputted password stored in printer memory that generates a number as a function of an input number, providing the same algorithm in a memory at a location secured from said printer, counting events of the printer that change dynamically as printing operations occur, determining the count of such events, and generating numbers separately using the algorithm in the printer and the algorithm at the location secure from the printer, and comparing such numbers as passwords for unlocking printer operations when a match occurs.

14. The process of claim 13 further including a drive computer for the printer, inputting the number generated at the algorithm secure from the printer

into the computer for comparison with the number generated by the printer memory for determining if printing operations should proceed.

15. The process of claim 13 and generating a number from the algorithm in the printer memory whenever a print command is provided to the printer and the printer remains unenabled.

16. The process of claim 13, wherein the number provided as an input to both of the algorithms is a number representing printing head passes made by the printer head at a selected time.

17. The process of claim 13, wherein the number provided as an input to both of the algorithms is a number representing items printed by the printer at a selected time.

18. The process of providing unique printing information keyed to a removable memory device key including providing a printer having memory capabilities and an encoding device coupled to the printer memory for encoding from an integrated circuit on a removable memory device key, using a host computer to input digital information onto the removable memory device key to provide commands to the printer, providing a password in the printer memory and on the removable memory device key, and printing the digital information from the removable memory device key only when the password on the removable memory device key and in the printer memory match.

19. A removable memory device key for a printer comprising a device having a programmable memory thereon, an encoder for encoding a password on the memory device, the password being used in connection with the printer for permitting operations of the printer when the password matches a password in the printer.

20. A printer having a memory therein and being operable in response to an unlocking code contained in the printer memory comprising a password, an encoder on said printer, having a portion that is externally accessible, and a removable memory device for associating with said encoding device, said removable memeory device carrying a programmable memory for receiving the password and subsequently for controlling printer operation only when the memory device is accessed to the encoder and the password in the printer memory is matched to the password of the removable memory device.

21. The printer of claim 20, wherein the printer has an access slot, and the device accesses the encoder by insertion into the slot.

FIG. 1

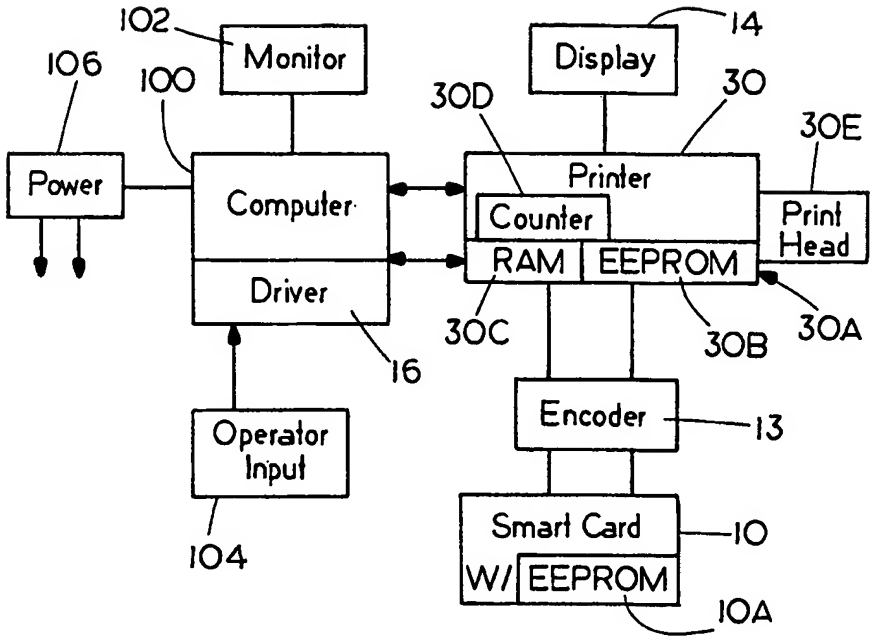

102
Monitor
106
100
Power
Computer
Driver
16
Operator Input
104
14
Display
30D
30
30E
Printer
Counter
Print Head
RAM
EEPROM
30C
30B
30A
Encoder
13
Smart Card
10
W/ EEPROM
10A

FIG. 2

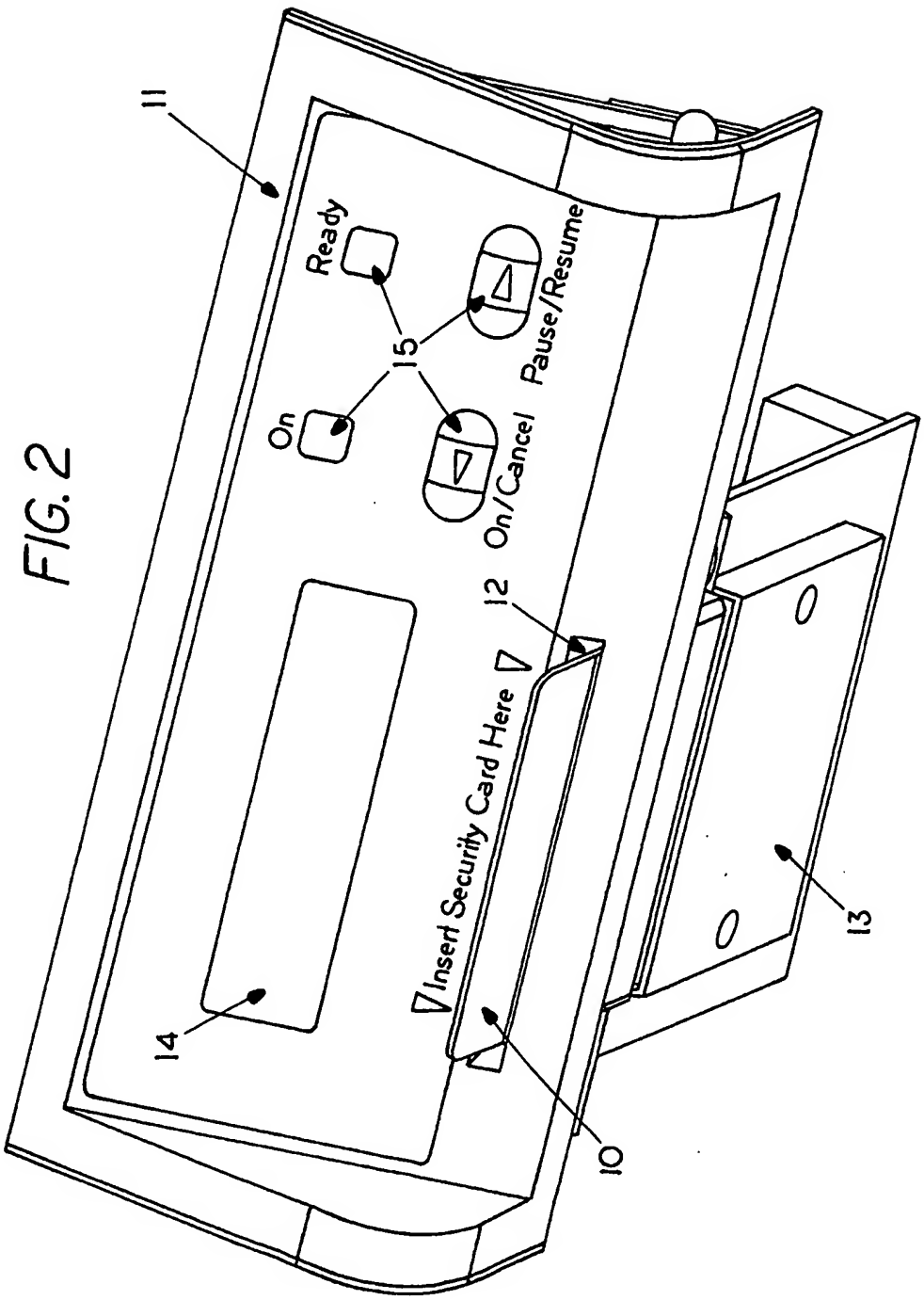

11
Ready
15
Pause/Resume
On
On/Cancel
12
Insert Security Card Here
14
10
13

FIG. 3

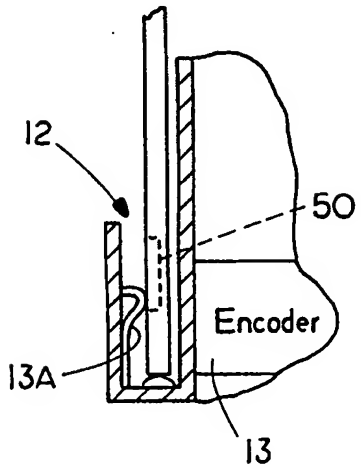


FIG. 4

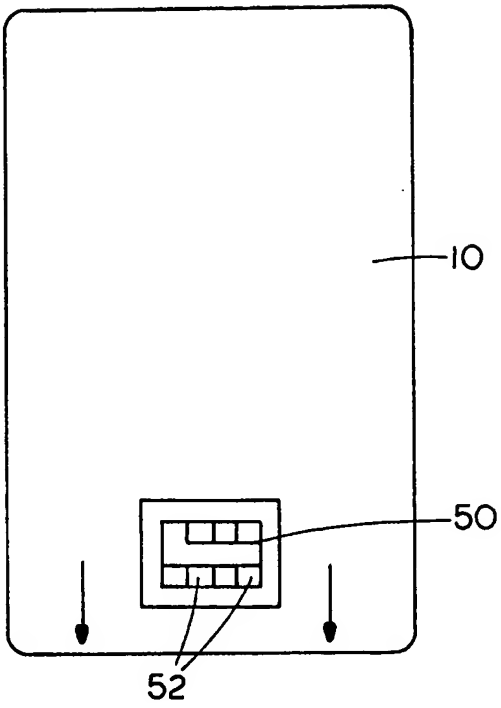


FIG. 5

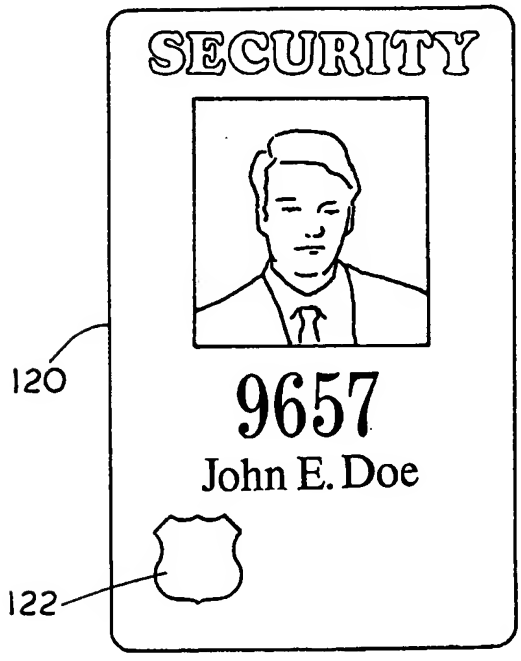


FIG.6

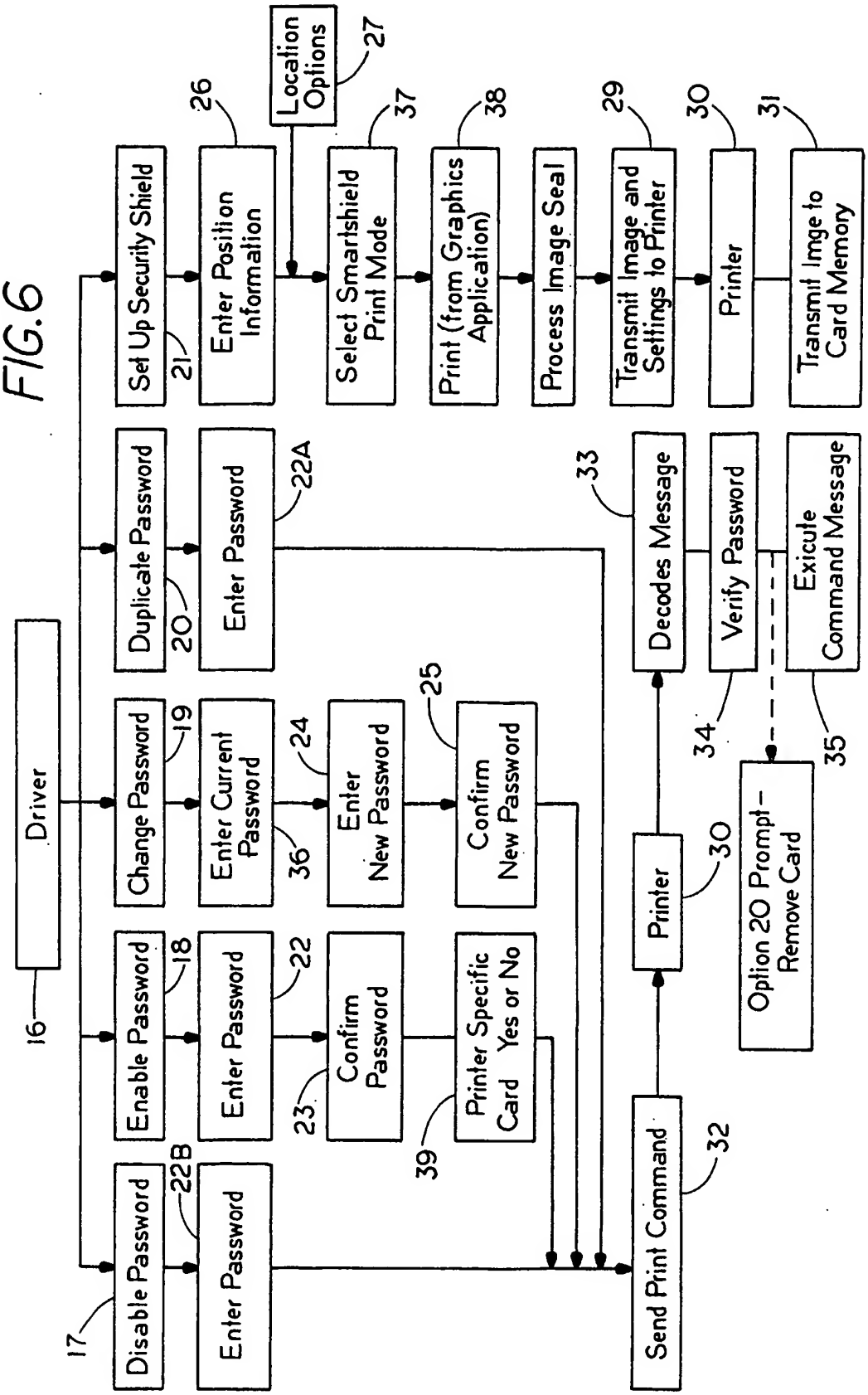

Driver
16
Disable Password
17
Enable Password
18
Change Password
19
Duplicate Password
20
Set Up Security Shield
21
Enter Password
22B
Enter Password
22
Confirm Password
23
Enter Current Password
24
Enter New Password
25
Confirm New Password
39
Printer Specific Card Yes or No
Enter Password
22A
Enter Position Information
26
Location Options
27
Select Smartshield Print Mode
37
Print (from Graphics Application)
38
Process Image Seal
Transmit Image and Settings to Printer
29
Printer
30
Transmit Imge to Card Memory
31
Decodes Message
33
Verify Password
34
Exicute Command Message
35
Option 20 Prompt - Remove Card
Printer
30
Send Print Command
32
36

FIG. 7

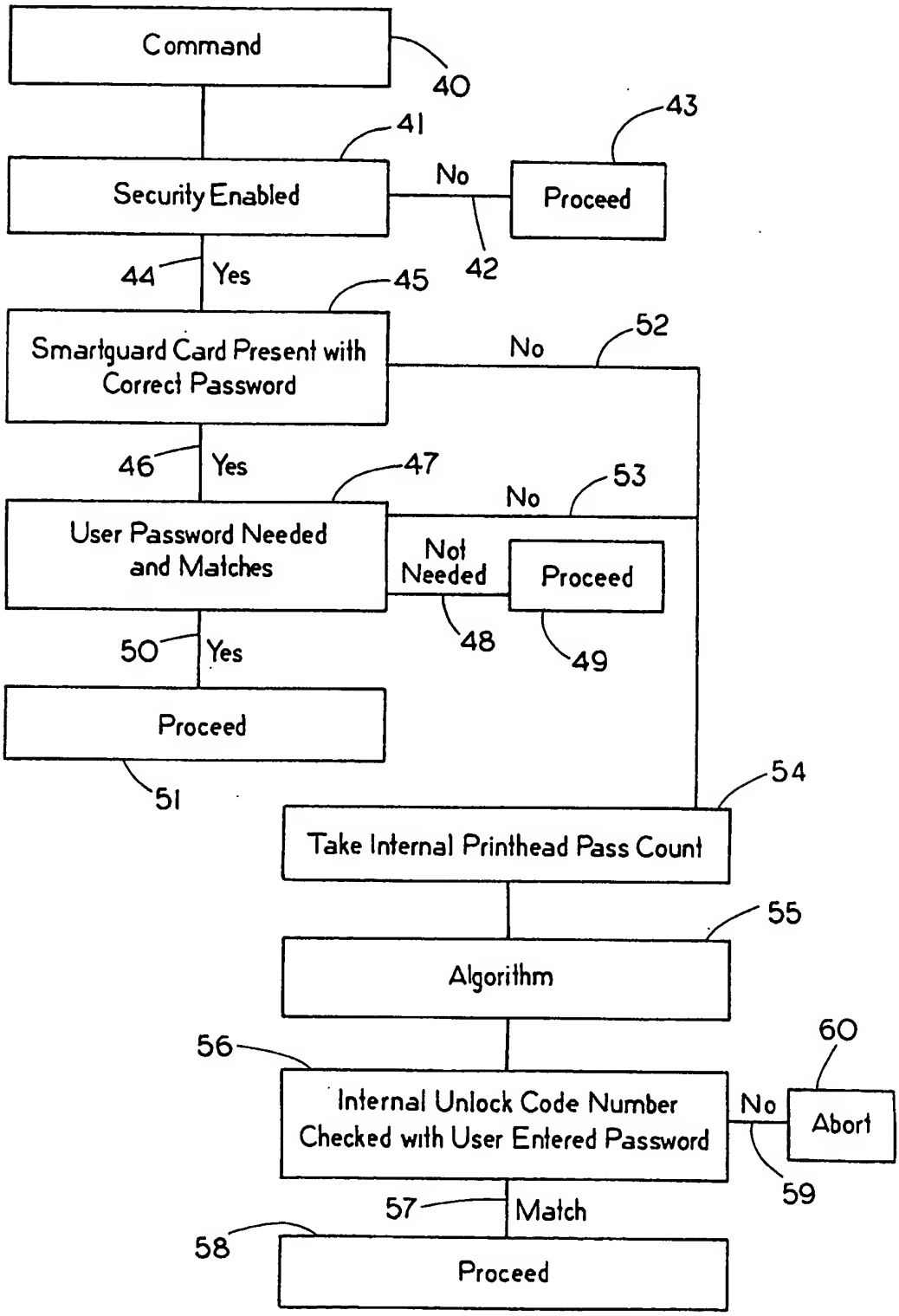
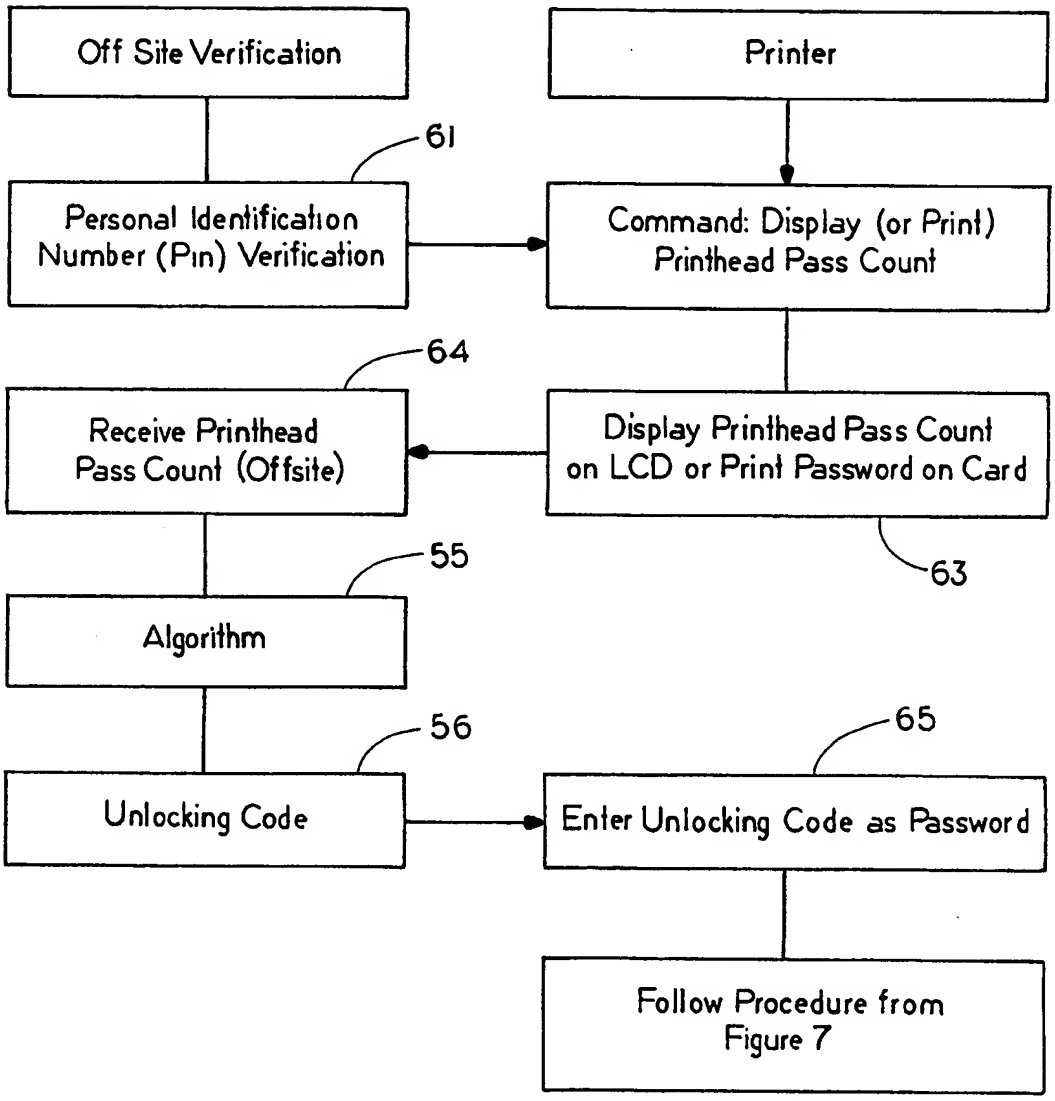

Command
40
41
Security Enabled
No
43
Proceed
42
44
Yes
45
Smartguard Card Present with Correct Password
No
52
46
Yes
47
User Password Needed and Matches
No
53
Not Needed
Proceed
48
49
50
Yes
Proceed
51
54
Take Internal Printhead Pass Count
55
Algorithm
56
60
Internal Unlock Code Number Checked with User Entered Password
No
Abort
59
57
Match
58
Proceed

FIG. 8


Off Site Verification
Printer
61
Personal Identification Number (Pin) Verification
Command: Display (or Print) Printhead Pass Count
64
Receive Printhead Pass Count (Offsite)
Display Printhead Pass Count on LCD or Print Password on Card
63
55
Algorithm
56
65
Unlocking Code
Enter Unlocking Code as Password
Follow Procedure from Figure 7

WLAN - IEEE 802.11

WPAN - Bluetooth

1

Lecture Outline

- Wireless Local Area Networks - IEEE 802.11
- Wireless Personal Area Networks - Bluetooth

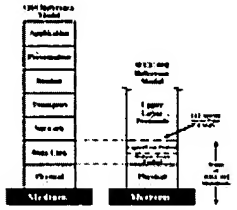
Based on the book: "Wireless communication and networks"

by © William Stallings, 2002 Prentice Hall

2

Wireless Local Area Networks

- Most known standard for WLAN - IEEE 802.11
- Use a layering architecture similar to OSI called IEEE 802 reference model



3

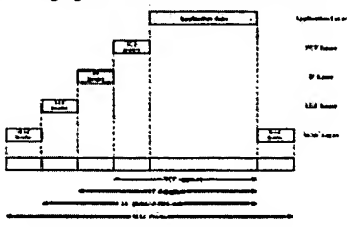
IEEE 802 Protocols Architecture

- Physical Layer:
  - encoding/decoding signals
  - generation/removal of synchronization data
  - transmission and reception of bits
  - include specifications of the transmission medium and topology
- Medium Access Control (MAC)
  - transmission is create data frames containing the original data and error correction and address information
  - reception is extract original data from the received message, perform address recognition and error detection
  - control access to the LAN transmission medium
- Logical Link Control (LLC)
  - provide interface to higher layers
  - perform flow and error control

4

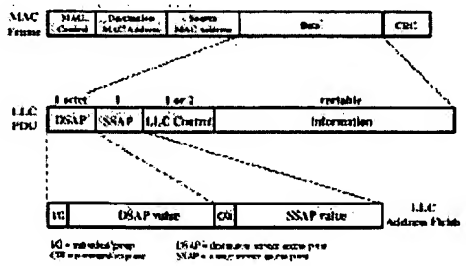
LLC and MAC

- Several MAC schemes can be used for LLC
- LLC needed since a traditional data link layer does not provide function for managing access to a shared-access medium



5

MAC Frame Format and LLC Protocol Data Unit (PDU)



6

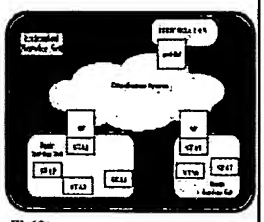
Logical Link Control

- Must support multiaccess
- Does not implement some details of link access due to MAC utilization
- LLC Services:
  - ***unacknowledged connectionless service***: no flow or error mechanisms, data delivery not guaranteed ⇙ ex: sensor networks
  - ***connection-mode service***: include flow and error control ⇙ ex: very simple devices
  - ***acknowledged connectionless service***: datagrams are acknowledged but no previous logical connection is established ⇙ automated factory including a central entity communicating with various devices

7

IEEE 802.11 Architecture

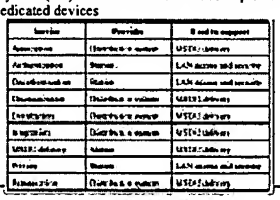
- Station: a device containing 802.11 equipment
- Basic Service Set (BSS): set of stations controlled by a coordination function
- Coordination function: logical function determining when a station can receive and send data in a BSS
- Distribution System (DS): a system connecting a set of BSS and integrated LANs to create an extended service set (ESS)
- Extended Service Set: a set of BSS and LANs appearing as a single unit to the LLC layer of the component stations
- Access point (AP) : entity providing access to the distribution system



8

IEEE 802.11 Services

- IEEE 802.11 define 9 services:
  - 6 services for supporting delivery of MAC service data units (MSDU) between stations
  - 3 services for LAN access and confidentiality
- Service provider type:
  - station: services implemented in stations and access point stations (APs)
  - distribution system (DS): services between BSSs implemented in access point stations or dedicated devices



9

Message distribution within the Distribution System (DS)

⇙ IEEE 802.11 define 2 services for message distribution in DS:

- Distribution Service
  - use to exchange MAC frames from stations in one BSS to stations in another BSS
  - if transmitting and receiving stations are within the same BSS-> the distribution service logically goes through the AP of the BSS
- Integration Service
  - transfer data between stations on an IEEE 802.11 network and stations on an integrated 802.X network (i.e. wired LAN physically connected with the DS)
  - deal with address translation and media conversion between the two networks

10

Association-Related Services [1]

- Provide information about stations within an extended service set (ESS)
- The distribution service can deliver or accept data only from ***associated*** stations -> DS need to know the location of the stations, i.e. the AP to which a message should be delivered for reaching further the destination
- Stations maintain association with the AP from their current BSS
- Three types of mobility are defined:
  - *No transition:* stationary stations or stations move only within the same BSS
  - *BSS transition:* stations may move from a BSS to another BSS within the same ESS
  - *ESS transition:* stations move from a BSS in one ESS to a BSS in another ESS

11

Association-Related Services [2]

⇙ IEEE 802.11 define 3 associated-related services:

- Association Service
  - establish initial association between a station and an AP
- Reassociation Service
  - enable an established association to be transferred from one AP to another when a station move from a BSS to another one
- Disassociation Service
  - association termination notice from station or from the AP associated with the station

12

Access and Privacy Services

- IEEE 802.11 define 3 access and privacy services:
  - Authentication Service
    - establish identity of stations to each other
    - can employ different schemes (e.g open system, shared key)
  - Deauthentication Service
    - invoked when existing authentication is terminated
  - Privacy Service
    - prevent message content from being read by non-intended recipients
    - optional encryption
    - use Wired Equivalent Privacy (WEP) algorithm

13

IEEE 802.11 Medium Access Control (MAC)

- IEEE 802.11 MAC cover 3 areas:
  - Reliable Data Delivery
    - require due to the error-prone wireless transmission characteristics
    - noise, interference, other propagation effects
  - Access Control
    - distributed access -> ad-hoc networks and networks implying bursty traffic
    - centralized access -> networks containing base stations connected with a backbone wired network
  - Security
    - require due to easing capturing transmission

14

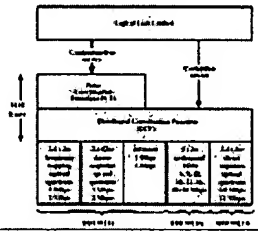
IEEE 802.11 MAC - Reliable Data Delivery

- MAC level:
  - more efficient to deal with errors at MAC than at higher layers
- IEEE 802.11 include a frame protocol
  - usually a two-frames protocol: data transmitted by the source station must be acknowledged (ACK) by the destination station
  - the exchange of Data+ACK is atomic -> not to be interrupted by other transmission
  - if the source does not receive ACK it retransmits the data
- IEEE 802.11 define a four-frame protocol for enhance reliability
  - source sends Request To Send (RTS) frame
  - destination responds with Clear To Send (CTS) frame
  - after receiving CTS, the source send data that must be acknowledged (ACK) by destination
  - RTS alert stations within source range about the current data exchange
  - CTS alert station within destination range about the current data exchange

15

IEEE 802.11 MAC - Access Control

- Distributed Foundation Wireless MAC (DFWMAC)
  - provide distributed access control with optional centralized control
  - Distributed Coordination Function (DCF) - use contention algorithm to provide access
  - Point Coordination Function (PCF) - centralized algorithm for contention-free services



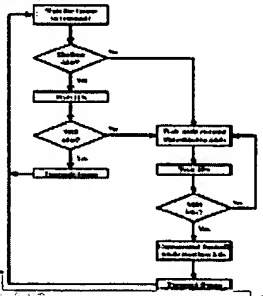
16

802.11 MAC - Distribution Coordination Function [1]

- Make use of CSMA (carrier sense multiple access)
- Use set of delays generic called Interframe Space (IFS)

Algorithm Logic:

1. *Station sense the medium*
2. *If medium idle, wait IFS, then if still idle transmit frame*
3. *If medium busy or become busy, defer and monitor the medium until idle*
4. *Then, delay IFS and sense medium*
5. *If medium idle, exponential backoff and if then if station transmit*

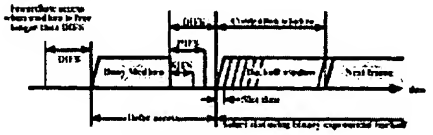


- Binary exponential backoff
  -> handle heavy load

17

802.11 MAC - Distribution Coordination Function [2]

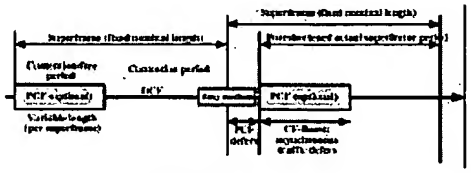
- Use 3 values for IFS:
  - SIFS (short IFS): shortest IFS used for immediate responses such as ACK, CTS, poll response
  - PIFS (point coordination function IFS): middle length IFS used for issuing polls by a centralized controller
  - DIFS (distributed coordination function IFS): longest IFS used for regular asynchronous frames



18

802.11 MAC - Point Coordination Function

- Alternative access method on top of DCF
- Polling operation by a centralized master
- Use PIFS when issuing polls
- For avoiding locking out the asynchronous traffic the superframe is used

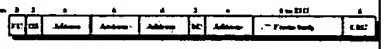


19

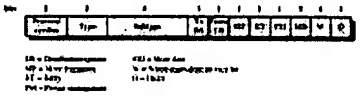
802.11 MAC - Frame Format

- Frame Control – frame type and control information
- Duration/connection ID – the time allocated for MAC frame transmission
- Addresses – include source, destination, transmitting and receiving station
- Sequence control – fragmentation/reassembly and numbering
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit CRC

- 802.11 MAC Frame



- 802.11 MAC Control Field



20

802.11 MAC - Frames Types

- ***Six types of control frames***
  - Power save - poll (PS-poll)
  - Request to send (RTS)
  - Clear to send (CTS)
  - Acknowledgment (ACK)
  - Contention-free (CF)-end
  - CF-end + CF-Ack
- ***Management frames***
  - association request and association response
  - reassociation request and reassociation response
  - probe request and probe response
  - beacon
  - announcement traffic indication message
  - disassociation
  - authentication and deauthentication
- ***Eight types of data frames***
  - *Carry user data*
    - Data
    - Data + CF-Ack
    - Data + CF-poll
    - Data + CF-Ack + CF-poll
  - *Do not carry user data*
    - Null Function
    - CF-Ack
    - CF-Poll
    - CF-Ack + CF-Poll

21

IEEE 802.11 MAC - Security

- Provide both privacy and authentication mechanisms
- Wired Equivalent Privacy (WEP) Algorithm:
  - modest protection
  - use encryption algorithm based on RC4
- Authentication:
  - open system authentication: identities exchange
  - shared key authentication: two parties share a key not shared by others

22

IEEE 802.11 issues

- Different IEEE 802.11 physical media
  - direct sequence spread spectrum (DS-SS)
  - frequency hopping spread spectrum (FH-SS)
  - infrared
- Currently well-known IEEE 802.11 versions
  - IEEE 802.11b: operating in ISM band, around 2.4 GHz, with data rates of 5.5 to 11 Mbps
  - IEEE 802.11a: operates in 5 GHz band with data rates of 6, 9, 12, .. 54 Mbps

23

Wireless Personal Area Network - Bluetooth

- Universal short-range wireless communication standard
- Up to 10 m indoor and 100 m outdoors
- Uses the ISM 2.4-GHz unlicensed band
- Data rate up to 720 kbps (asymmetric)
- Supports different applications: data transfer , audio, graphics, video, ...

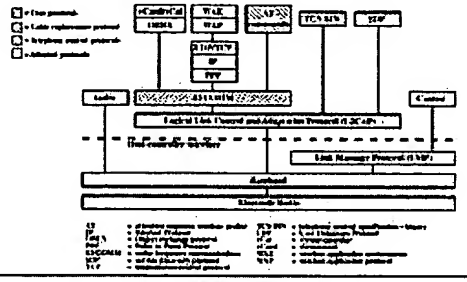
24

Bluetooth Applications Areas

- **Data and voice access points**: real-time voice and data transmissions to mobile and stationary devices
- **Cable replacement** eliminates need for cable attachments for connections
- **Ad hoc networking**: a Bluetooth device can establish spontaneous connection with another Bluetooth devices in the transmission range

Bluetooth Architecture [1]

- Core protocols
- Cable replacement and telephony protocols
- Adopted protocols

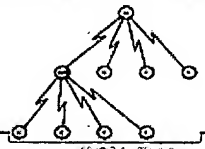


Bluetooth Core Protocols

- Radio:
  - specifies details related with the air interface utilization
  - include frequency hopping, modulation, encoding and transmission power
- Baseband:
  - connection establishment, addressing and packet format
  - power control and timing
- Link Manager Protocol (LMP):
  - link setup between devices and ongoing link management
  - include security, control and negotiation of baseband packets
- Logical Link Control and Adaptation Protocol (L2CAP):
  - adapts upper-layer protocols to baseband layer
  - provide connection-less and connection oriented services
- Service Discovery Protocol (SDP):
  - manage the query mechanisms for obtaining information about device services and characteristics of the services
  - connection may be established based on the collected data

Bluetooth Networking

- Piconets and Scatternets:
  - Bluetooth devices are organized in local networks called *piconets*
  - up to eight devices can be part of a piconet
  - devices are divided in *master* and *slaves*
  - the master control the utilization of the radio channel (e.g frequency-hopping sequence and timing) use in the communication with the slaves
  - a slave may communicate only with the master and when allowed by the master
  - a device may belong to different piconets and may be both a master and a slave in two different piconets
  - a network formed by several connected piconets is called a *scatternet*



Bluetooth Physical Links

- Synchronous Connection Oriented (SCO) links:
  - point-to-point connection between master and a single slave
  - allocates fixed bandwidth
  - the master maintains link using reserved slots (basic two slots, one per direction)
  - the master may support up to 3 SCO simultaneous links, a slave 2-3 SCO links
  - SCO packets are never retransmitted
  - used primarily for time-bounded data -> e.g. audio with built-in loss tolerance
- Asynchronous Connectionless (ACL) links:
  - point-to-multipoint link between master and all slaves
  - only single ACL link can exist
  - the master exchange data with slaves base on an per- slot basis
  - usually packet retransmission is applied
  - packet-switched style of connection
  - 1, 3 and 5 slot packets are defined

ACL Links Data Rates

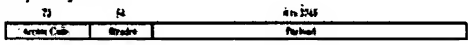
Type	Symmetric (kbps)	Asymmetric (kbps)	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	256.0	384.0	54.4
DH3	384.0	576.0	86.4
DM5	286.7	477.8	36.3
DH5	432.6	721.0	57.6

DMx = x-slot FEC-encoded
DHx = x-slot unprotected

Bluetooth Packets [1]

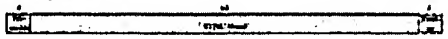
- Bluetooth specifies 15 types of packets [Stallings 15.3]

General packet format:



- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type and carry protocol control information
- Payload – contains user voice or data and usually a header and a CRC

Access code format:

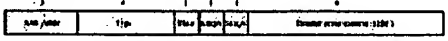


- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – paging and subsequent responses
- Inquiry access code (IAC) – inquiry purposes

31

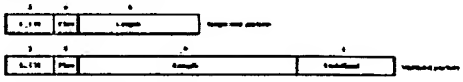
Bluetooth Packets [2]

Header format:



- AM_ADDR – contains "active mode" address of one of the slaves
- Type – identifies type of packet
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

Data payload header format:



- L_CH field – identifies logical channel
- Flow field – used to control flow at L2CAP level
- Length field – number of bytes of data

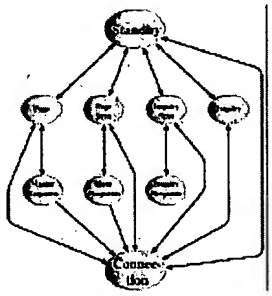
32

Bluetooth - Channel control in a piconet [1]

- Two major states of a Bluetooth device:
  - Standby: low-power state
  - Connection: the device is connected
- Seven states for adding new slaves to a piconet:
  - Page – device issued a page (used by master)
  - Page scan – device is listening for a page
  - Master response – master receives a page response from slave
  - Slave response – slave responds to a page from master
  - Inquiry – device has issued an inquiry for identity of devices within range
  - Inquiry scan – device is listening for an inquiry
  - Inquiry response – device receives an inquiry response

33

Bluetooth - Channel control in a piconet [2]



34

Bluetooth - Inquiry and Page Procedure

Inquiry Procedure:

- Potential master identifies devices in range that wish to participate
  - transmits an identification ID packet with inquiry access code (IAC)
  - occurs in Inquiry state
- Devices receives inquiry
  - enter Inquiry Response state
  - return data with address and timing information
  - moves to Page Scan state

Page Procedure

- Master uses devices address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with ID DAC packet
- Master responds with a special FHS packet
- Slave confirms receipt with DAC ID
- Slaves moves to Connection state

35

Bluetooth - Slave Connection State Modes

- Active – participates in piconet
  - listens, transmits and receives packets
- Sniff – only listens on specified slots
- Hold – does not support ACL packets
  - Reduced power status
  - May still participate in SCO exchanges
- Park – does not participate on piconet
  - Still retained as part of piconet

36

Bluetooth - Link Manager Protocol (LMP) Specification

- Manages various aspects of radio link between master and slaves
- Involve exchange of messages in form of LMP protocol data units (PDU)
- 24 functional areas for LMP procedures

LMP services

- Security: authentication, pairing, change link key, encryption ...
- Time/synchronization: clock offset request, slot offset information, timing accuracy information request
- Station capability: LMP version, supported features
- Mode control: switch master/slave role, name request, detach, hold mode, sniff mode, park mode, power control, QoS, SCO links, paging scheme, link supervision ...

Bluetooth - Logical Link Control and Adaptation Protocol (L2CAP) [1]

- Similar with LLC layer in IEEE 802.11
- Provide a number of services
- Make use of ACL links
- Provide two services for upper-layer protocols:
  - connectionless service: reliable datagram
  - connection-mode service: logical connection between two users that exchange data; include flow and error control
- L2CAP provide 3 types of logical channels:
  - connectionless: unidirectional, used typically for broadcast from master to slaves
  - connection-oriented: bidirectional with QoS specification assigned in each direction
  - signaling: exchange of signals between L2CAP entities

Bluetooth - Logical Link Control and Adaptation Protocol - Quality of Service (QoS)

- L2CAP defines flow specification: a set of parameters indicating the performance level that the transmitter should aim to achieve
- L2CAP flow specification parameters:
  - Service type: level of service (e.g. 1 = best effort; 2 = guaranteed service)
  - Token rate (bytes/second)
  - Token bucket size (bytes)
  - Peak bandwidth (bytes/second): limits how fast packets can be sent from applications
  - Latency (microseconds): maximum acceptable delay
  - Delay variation (microseconds): difference between maximum and minimum delay of a packet

Lecture Summary

- Brief description of IEEE 802.11: standard, layering, architecture, services, MAC, LLC, security
- Brief description of Bluetooth: standard, applications, architecture, packet format, networking, channel control in piconets, LMP, L2CAP